

# Chapitre :

# Divisibilité



⊗ **Activité** : page 7 (sauf C ?)

## I. Divisibilité dans $\mathbb{Z}$

---

⊗ **Activité** : 1p8

**Définition** Soit  $a$  et  $b$  deux entiers (relatifs). On dit que  $a$  divise  $b$  si et seulement si il existe un entier  $k$  tel que  $b = ka$ . On dit aussi que  $a$  est un diviseur de  $b$  ou que  $b$  est un multiple de  $a$ .

**Exemple** 7 divise  $-21$  car  $-21 = (-3) \times 7$ .

**Remarque** Évidemment,  $a$  et  $-a$  ont les mêmes diviseurs. Le plus souvent on ne s'intéresse qu'aux diviseurs des (nombres entiers) naturels, donc à la divisibilité dans  $\mathbb{N}$ .

### Propriété

1. Tout diviseur positif d'un entier naturel non nul  $n$  est compris entre 1 et  $n$ .
2. Tout naturel non nul a un nombre fini de diviseurs ;

**Preuve :**

1. On peut raisonner par l'absurde. Supposons que  $n$  a un diviseur  $d$  qui est strictement supérieur à  $n$ . Il existe un entier  $k$  tel que  $n = k \times d$ . Comme  $n > 0$  ainsi que  $d$ , on a nécessairement  $k \geq 1$  et donc  $k \times d \geq d > n$ . Ceci est contradictoire.
2. Cela découle directement de la première partie, si ce n'est qu'il faut compter les diviseurs négatifs, ce qui en fait au plus  $2n$  ( $0$  n'est pas un diviseur).

□

**Remarque** 0 a lui une infinité de diviseurs : tout nombre divise 0.

**Exemple** Pour les nombres raisonnables, on peut alors donner l'ensemble de leurs diviseurs.

–  $\mathcal{D}(6) = \{-6; -3; -2; -1; 1; 2; 3; 6\}$

–  $\mathcal{D}(7) = \{-7; -1; 1; 7\}$

En général on se contente de donner les diviseurs positifs.

**Exemple** Voir les exercices corrigé 1, 2 et 3 page 11.

► **Exercices** : 1-9 page 24

### Propriété

1. 1 divise  $a$  pour tout entier  $a$  ;

2.  $a$  divise  $a$  pour tout entier  $a$  ;
3. Si  $a$  divise  $b$  et  $b$  divise  $c$ , alors  $a$  divise  $c$ . On dit que la relation de divisibilité est transitive ;
4. Si  $a$  divise  $b$  et  $m$  est un entier, alors  $a$  divise  $mb$  ;
5. Si  $a$  divise  $b$  et  $c$ , alors  $a$  divise  $b + c$  et plus généralement  $mb + nc$  avec  $m$  et  $n$  entiers.

**Preuve :** Simple utilisation de la définition □

**Définition** On appelle équation diophantienne toute équation dont les constantes et les inconnues sont des nombres entiers.

**Exemple** –  $x^2 = 3$  n'a pas de solution, alors que  $x^2 = 4$  a deux solutions ( $-2$  et  $2$ )

– Le plus souvent il y a plus d'inconnues que d'équations :  $x + y = 5$ . Il peut y avoir une infinité de solution (ici c'est le cas sur  $\mathbb{Z}$ ) ou un nombre fini de solutions (ici c'est le cas sur  $\mathbb{N}$ ).

**Exemple** Voir l'exercice corrigé page 11

► **Exercices :** 10-15 page 24

## II. Division euclidienne des entiers

---

⊗ **Activité** : 3p9

**Propriété** | Soit  $a$  un entier et  $b$  un entier naturel non nul. Il existe un unique entier  $q$  et un unique entier  $r$  tels que

$$a = bq + r, \text{ avec } 0 \leq r < b$$

**Preuve** :

- Si  $b$  divise  $a$ , alors il existe un entier  $q$  tel que  $a = bq$ . On pose  $r = 0$ , on a alors l'égalité souhaitée.
- Sinon,  $a$  est encadré par deux multiples successifs de  $b$ , ce que l'on peut noter :

$$bq < a < b(q + 1)$$

avec  $q$  entier déterminé de manière unique.

On a alors

$$0 < a - bq < b$$

en soustrayant par  $bq$ . En posant  $r = a - bq$  (unique par unicité de  $q$ ), on a :

$$a = bq + (a - bq) = bq + r$$

□

On dit que  $q$  est le quotient et que  $r$  est le reste de la division euclidienne de  $a$  par  $b$ .

**Exemple** La division euclidienne de  $-47$  par  $7$  donne :

$$-47 = 7 \times (-7) + 2$$

Celle de  $47$  par  $7$  donne :

$$47 = 7 \times 6 + 5$$

**Exemple** L'égalité  $55 = 6 \times 8 + 7$  peut être vu comme la division euclidienne de  $55$  par  $8$  mais pas comme celle de  $55$  par  $6$  (car le reste doit être inférieur au diviseur)

La division euclidienne de  $55$  par  $6$  donne

$$55 = 6 \times 9 + 1$$

**Remarque** Le reste de la division euclidienne d'un nombre  $n$  par  $2$  est soit  $0$  soit  $1$ , donc tout entier  $n$  s'écrit soit  $2k$ , soit  $2k + 1$  avec  $k$  entier.

Avec le même raisonnement avec la division par  $3$ , tout nombre s'écrit soit  $3k$ , soit  $3k + 1$ , soit  $3k + 2$  avec  $k$  entier.

**Remarque**

- On peut observer que  $b$  divise  $a$  si et seulement si le reste de la division euclidienne de  $a$  par  $b$  vaut  $0$ .
- Si l'on considère que  $b \in \mathbb{Z}$ , alors le résultat est le même avec  $0 \leq r < |b|$ .

Lire L'exercice corrigé 2p13

► Exercices : 22,24,25p24

► Exercices : 26-32p25

► Exercices : 34-37p24 ?

## III. Nombres premier

---

**Définition** Un nombre premier est un nombre entier naturel qui a exactement deux diviseurs dans  $\mathbb{N}$ , 1 et lui-même.

**Remarque** Cette définition exclut le nombre 1, et le plus petit nombre premier est 2.

- Propriété** | 1. Tout nombre entier supérieur à 1 a au moins un diviseur premier.
2. Tout nombre entier  $n$  supérieur à 1 non premier admet au moins un diviseur premier  $p$  tel que  $p \leq \sqrt{n}$ .
3. Il y a une infinité de nombres premiers.

**Preuve :**

1. Soit  $n$  un entier supérieur à 1. Considérons le plus petit diviseur  $p$  de  $n$  supérieur à 1. Alors  $p$  est premier car sinon il admettrait un diviseur  $d$  tel que  $1 < d < p$ . Or, par transitivité,  $d$  serait un diviseur de  $n$  inférieur à  $p$  ce qui serait contradictoire.
2. Soit  $n > 1$  et  $p$  le plus petit diviseur (premier d'après le point précédent) de  $n$ , il existe  $q$  tel que  $n = qp$ . Alors  $q$  est un diviseur de  $n$ , et on a donc  $p \leq q$ . Par suite,  $p^2 \leq qp = n$ . La fonction carré étant croissante sur  $\mathbb{R}^+$ , on obtient que  $p \leq \sqrt{n}$ .
3. On prouve cela par l'absurde, en supposant donc qu'il y ait un nombre fini de nombres premiers, notés  $p_1, \dots, p_n$ . Considérons le nombre :

$$P = \prod_{i=1}^n p_i + 1$$

$P$  est supérieur à 1 donc il admet un diviseur premier  $p$ , qui est nécessairement dans la liste  $p_1, \dots, p_n$ . Or la division euclidienne de  $P$  par  $p$  est 1 d'après la définition de  $P$  et non 0 : contradictoire.

□

**Propriété** | Soit  $n$  un entier naturel supérieur ou égal à 2. Si  $n$  n'admet pas de diviseur premier  $p$  tel que  $p \leq \sqrt{n}$ , alors  $n$  est premier.

Autrement dit, pour savoir si un nombre  $n$  est premier, il suffit de tester la divisibilité de  $n$  par les nombres premiers  $p$  tels que  $p \leq \sqrt{n}$ .

**Preuve :** Cette propriété n'est que la contraposée de la propriété 2 ci-dessus.

**Voir** page 15 (dont crible d'Erathostène)

► Exercices : 38,39,43,45 ?,46p25

► Exercices : 52p26

**Théorème** | Tout entier naturel supérieur à 1 se décompose en produit de facteurs premiers et cette décomposition est unique (à l'ordre des facteurs près).

**Preuve :** On admet ici l'unicité, mais on prouve l'existence. La récurrence permet une preuve rapide.  
□

**Propriété** | Soit  $d$  et  $n$  deux entiers naturels supérieurs à 1. Alors  $d$  divise  $n$  si et seulement si tous les nombres premiers de la décomposition en produit de nombres premiers de  $d$  se retrouvent dans celle de  $n$  avec un exposant au plus égal.

**Preuve :**

- Supposons que  $d$  divise  $n$ . Alors il existe un entier  $q$  tel que  $n = qd$ . En utilisant la décomposition en produit de nombres premiers de  $d$ , on observe la conclusion de la propriété.
- Réciproquement, on suppose que tous les nombres premiers de [...]. En écrivant les décompositions de  $n$  et de  $d$ , on observe que  $n = dq$ , donc que  $d$  divise  $n$ .

□

Voir page 17

► **Exercices :** 54,55,57,59p26

# IV. Congruences

---

⊗ **Activité** : fiche

## 1. Définitions

Deux entiers  $a$  et  $b$  sont congrus modulo un entier naturel  $n$  si  $a$  et  $b$  ont le même reste dans la division euclidienne par  $n$ .

On dit aussi que  $a$  est congru à  $b$  modulo  $n$ , et on le note  $a \equiv b[n]$  (au lieu des crochets on peut utiliser des parenthèses).

**Théorème** | Soit  $a, b$  deux entiers et  $n$  un entier naturel. Les deux propositions suivantes sont équivalentes :

- $a \equiv b[n]$
- $a - b$  est divisible par  $n$

**Preuve** :

□

## 2. Propriétés

**Propriété** |

- $a$  est divisible par  $n$  si et seulement si  $a \equiv 0[n]$  ;
- $n \equiv 0[n]$  ;
- $a \equiv a[n]$  ;
- Si  $a \equiv b[n]$  et  $b \equiv c[n]$ , alors  $a \equiv c[n]$  (transitivité) ;
- Si  $a \equiv b[n]$  et  $a' \equiv b'[n]$ , alors  $a + a' \equiv b + b'[n]$  ;
- Si  $a \equiv b[n]$  et  $a' \equiv b'[n]$ , alors  $aa' \equiv bb'[n]$  ;
- Si  $a \equiv b[n]$  et  $p \in \mathbb{N}^*$ , alors  $a^p \equiv b^p[n]$ .

**Preuve** : Les seules propriétés qui nécessitent d'utiliser les définitions dans le détail sont les deux dernières. □

## 3. Utilité

### (a) Critères de divisibilité

On est maintenant en mesure de démontrer très simplement les critères de divisibilité connus depuis longtemps :

**Propriété** |

- Un entier est divisible par 10 s'il se termine par 0.
- Un entier est divisible par 5 s'il se termine par 0 ou 5.
- Un entier est divisible par 2 s'il se termine par un chiffre pair (0, 2, 4, 6 ou 8).
- Un entier est divisible par 3 si la somme des chiffres qui le compose est divisible par 3.
- Un entier est divisible par 9 si la somme des chiffres qui le compose est divisible par 9.

- Un entier est divisible par 4 si le nombre formé par les deux derniers chiffres du nombre est divisible par 4.

**Preuve :** On utilise la notation  $n = \overline{a_n a_{n-1} \dots a_1 a_0}$  où les  $a_i$  sont des chiffres pour signifier que  $n = a_n \times 10^n + a_{n-1} \times 10^{n-1} + \dots + a_1 \times 10 + a_0$ .

On utilise les propriétés vues précédemment pour savoir à quoi est congru un nombre  $n$  avec les nombres dont on connaît les critères de divisibilité.  $\square$

- ▶ **Exercices :** page 27
- ▶ **Exercices :** 125,126,127,128p29
- ▶ **Exercices :** pages 30 et 31
- ▶ **Exercice :** en salle informatique : p33

# V. PGCD et PPCM

---

## 1. PGCD

⊗ **Activité** : 1

**Définition** Soit  $a$  et  $b$  deux entiers naturels non nuls. Le plus grand élément de l'ensemble  $\mathcal{D}(a) \cap \mathcal{D}(b)$  des diviseurs communs de  $a$  et de  $b$ , est appelé le **plus grand commun diviseur** de  $a$  et  $b$ , ou encore PGCD de  $a$  et  $b$ .

On peut le noter  $\text{pgcd}(a, b)$ .

**Exemple**  $\text{pgcd}(a, a) = a$  ;  $\text{pgcd}(a; 1) = 1$ .

On considère que le PGCD de  $a$  et de 0 est  $a$ , car  $\mathcal{D}(0) = \mathbb{N}$ .

**Propriété** Soit  $a$  et  $b$  deux entiers au moins égaux à 2. Le PGCD de  $a$  et  $b$  est égal au produit des facteurs premiers communs de  $a$  et  $b$ , avec pour chacun d'eux l'exposant le plus petit de ceux qu'il a dans  $a$  et dans  $b$ .

**Preuve** : Elle n'est pas très intéressante. □

D'ailleurs cette propriété ne donne pas un moyen très pratique de déterminer le PGCD de deux nombres.

**Exemple** Le PGCD de  $252 = 2^2 \times 3^2 \times 7$  et  $120 = 2^3 \times 3 \times 5$  est  $2^2 \times 3 = 12$ .

**Propriété**

1. Si  $a$  divise  $b$ , alors  $\text{pgcd}(a, b) = a$ .

2. (propriété fondamentale) Soit  $a$  non nul tel que  $a = bk + r$ .

Alors les diviseurs communs de  $a$  et  $b$  sont les mêmes que ceux de  $b$  et  $r$ .

Par conséquent,  $\text{pgcd}(a, b) = \text{pgcd}(b, r) = \text{pgcd}(b, a - bk)$ .

Cette propriété est à la base de l'algorithme d'Euclide.

**Preuve** : Le premier point étant évident, démontrons le second.

Soit  $d$  un diviseur commun de  $a$  et  $b$ . Démontrons que  $d$  divise aussi  $r$ . On a  $a = da'$  et  $b = db'$ , ainsi  $r = a - bk = da' - db'k = d(a' - b'k)$ , donc  $d$  divise  $r$ .

Réciproquement, soit  $d$  un diviseur commun de  $b$  et  $r$ . Alors  $d$  divise aussi  $a$  par le même type de raisonnement.

On vient de démontrer que les deux ensembles sont égaux. Ainsi, ils ont le même plus grand élément, ce qui se traduit par  $\text{pgcd}(a, b) = \text{pgcd}(b, r)$ . □

**Remarque** En particulier  $\text{pgcd}(a, b) = \text{pgcd}(b, a + b)$ .



► Exercices : 1,3,4,5,7 p55

## 2. Algorithme d'Euclide

On rappelle l'algorithme d'Euclide vu en sixième : on effectue des divisions euclidiennes successives en commençant par  $a$  et  $b$ , puis en continuant successivement par les diviseurs et restes.

**Propriété** | Le dernier reste non nul obtenu par l'algorithme d'Euclide appliqué à  $a$  et  $b$  est le PGCD de  $a$  et de  $b$ .

### Corollaire

1. L'ensemble des diviseurs communs à 2 entiers  $a$  et  $b$  est l'ensemble des diviseurs de leur PGCD.
2. Soit  $a$  et  $b$  des entiers non nuls et  $k$  un entier non nul. Alors

$$\text{pgdc}(ka, kb) = k \text{ pgcd}(a, b)$$

**Preuve** : Voir le livre. □

► Exercices : 8,10,11,13,14,15p55

## 3. Théorème de Bézout

**Définition** Deux entiers sont premiers entre eux lorsque leur PGCD est égal à 1.

**Propriété** | Soit  $a$  et  $b$  des entiers naturels non nuls et  $d$  un diviseur commun de  $a$  et  $b$ . On pose  $a = da'$  et  $b = db'$ . Le PGCD de  $a$  et  $b$  est  $d$  si et seulement si  $a'$  et  $b'$  sont premiers entre eux.

**Preuve** : Si  $d$  est le PGCD de  $a$  et  $b$ , en utilisant les propriétés précédentes on a :

$$d = \text{pgcd}(a, b) = \text{pgcd}(da', db') = d \times \text{pgcd}(a', b')$$

Or,  $d$  étant non nul, on en déduit que  $\text{pgcd}(a', b') = 1$  :  $a'$  et  $b'$  sont premiers entre eux. Réciproquement, Si  $a'$  et  $b'$  sont premiers entre eux,

$$\text{pgcd}(a, b) = \text{pgcd}(da', db') = d \times \text{pgcd}(a', b') = d \times 1 = d$$

□

**Théorème** | (**de Bézout**) Deux entiers  $a$  et  $b$  sont premiers entre eux si et seulement si il existe des entiers  $u$  et  $v$  tels que  $au + bv = 1$ .

**Preuve** :

- On suppose  $a$  et  $b$  premiers entre eux. Alors  $\text{pgcd}(a, b) = 1$ . En particulier l'un des deux nombres  $a$  et  $b$  est non nul. Supposons par exemple que  $a \neq 0$ . Considérons l'ensemble  $\mathcal{E}$  des nombres  $d$  qui s'écrivent sous la forme  $d = au + bv$ . Cet ensemble est non vide et contient au moins un nombre non nul positif :  $a$  ( $u = 1$  et  $v = 0$ ).

Soit  $d$  le plus petit entier positif de cet ensemble. Il existe donc  $u$  et  $v$  tels que  $au + bv = d$  ( $E$ ).

En considérant la division euclidienne de  $a$  par  $d$ , on peut écrire  $a = dq_a + r_a$  avec  $0 \leq r_a < d$ .

Par suite, ( $E$ ) implique  $auq_a + bvq_a + r_a = dq_a + r_a = a$ , ce qui équivaut à  $r_a = a(1 - uq_a) - bvq_a$ .

Autrement dit,  $r_a$  est dans l'ensemble  $\mathcal{E}$ . Mais comme  $r_a$  est strictement inférieur à  $d$  et positif, et que  $d$  est minimal dans  $\mathcal{E}$ , on en déduit que  $r_a = 0$ . Autrement dit,  $d$  divise  $a$ .

On démontre de manière similaire que  $d$  divise  $b$ . Or  $a$  et  $b$  sont premiers entre eux. Cela démontre que  $d = 1$ .

- Réciproquement, si il existe  $u$  et  $v$  tels que  $au + bv = 1$ , soit  $d = \text{pgcd}(a, b)$ . Alors  $d$  divise  $a$  et  $b$ , donc la somme  $au + bv$ , qui vaut 1. Donc  $d = 1$  :  $a$  et  $b$  sont premiers entre eux.  $\square$

**Exemple** On considère les nombres 8 et 15, qui sont premiers entre eux. Cherchons  $u$  et  $v$  tels que  $8u + 15v = 1$ .

On peut trouver par tâtonnement :  $2 \times 8 - 15 = 16 - 15 = 1$ , donc  $u = 2$  et  $v = -1$ .

Sinon, on peut utiliser l'algorithme d'Euclide :

$$15 = 1 \times 8 + 7 \quad ; \quad 8 = 1 \times 7 + 1$$


On a donc :

$$1 = 8 - 1 \times 7 = 8 - 1 \times (15 - 1 \times 8) = 8 - 1 \times 15 + 1 \times 8 = 2 \times 8 - 1 \times 15$$

**Remarque** Grâce à l'équivalence, on en déduit que  $u$  et  $v$  sont donc eux aussi premiers entre eux ! (ainsi que  $a$  et  $v$  et que  $u$  et  $b$ ).

**Corollaire** | Soit  $a$  et  $b$  deux entiers et soit  $d = \text{pgcd}(a, b)$ . Alors il existe deux entiers  $u$  et  $v$  tels que  $au + bv = d$ .

**Preuve** : En notant  $a = da'$  et  $b = db'$ , on sait que  $a'$  et  $b'$  sont premiers entre eux. Alors il existe  $u'$  et  $v'$  tels que  $a'u' + b'v' = 1$ . En multipliant par  $d$ , et en posant  $u = du'$  et  $v = dv'$ , on obtient bien  $au + bv = d$ .  $\square$

 La réciproque est fautive : si  $au + bv = d$ ,  $d$  n'est pas nécessairement le PGCD de  $a$  et  $b$ . Par exemple,  $2 \times 5 + (-1) \times 7 = 3$ , mais 3 n'est pas le PGCD de 5 et 7.

► **Exercices** : 16,17,19,20 (sauf la réciproque, pour plus tard),24p55

► **Exercices** : 28,29,38p56

**Propriété** | Un nombre premier est premier avec tous les nombres qu'il ne divise pas.

**Preuve** : Exercice.  $\square$

**Propriété** | Si un entier est premier avec deux entiers, alors il est premier avec leur produit.

**Preuve** : Soit  $a$  entier premier avec  $b$  et avec  $b'$ . On doit démontrer que  $a$  est premier avec  $bb'$ .

Or, il existe  $u, v, u'$  et  $v'$  tels que  $au + bv = 1$  et  $au' + b'v' = 1$ .

Ainsi, on a l'égalité  $bv = 1bv = (au' + b'v')bv$ . Par suite,

$$au + bv = au + (au' + b'v')bv = a(u + u') + bb'(v'v) = 1$$

Ainsi,  $a$  et  $bb'$  sont bien premiers.  $\square$

## 4. Théorème de Gauss

**Théorème** | (**De Gauss**) Soit  $a, b$  et  $c$  trois entiers. Si  $a$  divise le produit  $bc$  et si  $a$  et  $b$  sont premiers entre eux, alors  $a$  divise  $c$ .

**Preuve** : Il existe  $u$  et  $v$  tels que  $au + bv = 1$ , et donc  $acu + bcv = c$ . Or,  $a$  divise  $bc$ , donc  $bc = qa$ . Par suite,  $a(cu + qv) = c$ . Autrement dit,  $a$  divise  $c$ .  $\square$

### Corollaire

1. Si un entier est divisible par des entiers  $a$  et  $b$  premiers entre eux, alors il est divisible par le produit  $ab$ .
2. Si un entier premier divise un produit de facteurs  $ab$ , alors il divise au moins des facteurs  $a$  et  $b$ .

### Preuve :

1. On écrit  $n = pa = qb$  ( $n$  est divisible par  $a$  et  $b$ ). On en déduit que  $a$  divise  $qb$ . Or  $a$  et  $b$  sont premiers entre eux, donc  $a$  divise  $q$ . Autrement dit, on peut écrire  $q = ka$ . Ainsi,  $n = qb = kab$  :  $ab$  divise  $n$ .
2. Soit  $p$  un nombre premier qui divise  $ab$ . Si  $p$  ne divise pas  $a$ , alors  $p$  et  $a$  sont premiers entre eux. Par suite,  $p$  divise  $b$ .  $\square$

**Application :** Résolution d'équations de la forme  $ax + by = c$  ( $x$  et  $y$  entiers).

**Exemple** Pour résoudre  $2x + 3y = 5$ , on commence par résoudre  $2x + 3y = 1$ . Pour cela, on cherche une solution particulière.

Ici, le couple  $(2; -1)$  est une solution particulière. On a donc :

$$\begin{cases} 2x + 3y = 1 \\ 2 \times 2 + 3 \times (-1) = 1 \end{cases}$$

En soustrayant terme à terme, on obtient  $2(x - 2) + 3(y + 1) = 0$ , soit  $2(2 - x) = 3(y + 1)$  ( $E$ ). Ainsi, 2 divise  $3(y + 1)$ . Or 2 et 3 sont premiers entre eux, donc 2 divise  $y + 1$ . Il existe un entier  $k$  tel que  $y + 1 = 2k$ .

En remplaçant dans l'équation ( $E$ ),  $2 - x = 3k \Leftrightarrow x = 2 - 3k$

Ainsi, les couples  $(2 - 3k; 2k - 1)$ , pour  $k$  entier, sont solution de l'équation.

► **Exercices :** 39,41,43,44,45,50p56 (équations de type  $ax + by = c$ ) et 52p57

► **Exercices :** 57,59,61,65p57 (utilisation du corollaire)

► **Exercices :** 68p57

## 5. PPCM

⊗ **Activité** : 3.1 page 41 (synchronisation de feux)

► **Exercice** : Acti 3.2 en DM

**Définition** Le plus petit multiple de deux entiers naturels  $a$  et  $b$  est le plus petit élément de  $\mathcal{M}(a) \cap \mathcal{M}(b)$ , ensemble des multiples communs de  $a$  et de  $b$ . On l'appelle aussi PPCM de  $a$  et  $b$  ou  $\text{ppcm}(a, b)$ .

**Exemple**  $\text{ppcm}(1; a) = a$ ;  $\text{ppcm}(0; a) = 0$ .

**Propriété** Le PPCM de deux entiers  $a$  et  $b$  est égal au produit des facteurs premiers de  $a$  et de  $b$ , avec pour chacun d'eux la plus grande puissance qu'il a dans  $a$  ou dans  $b$ .

**Preuve** : Voir le livre. □

**Exemple** On a  $90 = 2 \times 3^2 \times 5$  et  $95 = 5 \times 19$ . Ainsi,  $\text{ppcm}(90; 95) = 2 \times 3^2 \times 5 \times 19$ .

De même que pour le PGCD, cette méthode n'est pas très pratique en général. On utilise alors la propriété suivante :

### Propriété

1. L'ensemble des multiples communs de  $a$  et  $b$  est l'ensemble des multiples de leur PPCM.
2. On a l'égalité suivante :

$$\text{ppcm}(a; b) \times \text{pgcd}(a; b) = a \times b$$

3. En conséquence, grâce à la propriété sur le PGCD,  $\text{ppcm}(ka, kb) = k \times \text{ppcm}(a, b)$ .

**Preuve** : Il suffit de « compter » les facteurs premiers de chaque côté. □

Ainsi, pour obtenir le PPCM, il suffit par exemple de déterminer le PGCD (par l'algorithme d'Euclide), puis on utilise la formule pour obtenir le PPCM.

► **Exercices** : 70,73,75p58

## 6. Petit théorème de Fermat

**Propriété** Soit  $p$  un nombre premier et  $1 \leq i \leq p-1$ . Alors  $p$  divise  $\binom{p}{i}$ .

**Preuve** : La formule du coefficient binomial est  $\binom{p}{i} = \frac{p(p-1)\dots(p-i+1)}{i!}$ . On a donc l'égalité suivante (de nombres entiers) :

$$i! \times \binom{p}{i} = p(p-1)\dots(p-i+1)$$

Ainsi,  $p$  divise  $i! \times \binom{p}{i}$ . Or,  $p$  est premier, donc premier avec tous les facteurs de  $i!$  (car  $1 \leq i \leq p-1$ ). Le théorème de Gauss permet alors de conclure. □

**Théorème** | Si  $p$  est un nombre premier et  $n$  un entier, alors

$$n^p \equiv n \quad [p]$$

**Preuve** : Elle se fait par récurrence sur  $n$ . C'est évidemment vrai pour  $n = 0$ . Pour l'étape de récurrence, on utilise la formule de Newton :

$$(n + 1)^p = \sum_{i=0}^p \binom{p}{i} n^i$$

En utilisant la propriété précédente, on obtient alors (seuls  $i = 0$  et  $i = p$  ne sont pas concernés par la propriété) :

$$(n + 1)^p \equiv \binom{p}{0} n^0 + \binom{p}{p} n^p \quad [p]$$

Soit

$$(n + 1)^p \equiv 1 + n^p \quad [p]$$

L'hypothèse de récurrence permet de conclure. □

**Théorème** | (**Petit théorème de Fermat**) Soit  $n$  un entier et  $p$  un nombre premier ne divisant pas  $n$ . Alors

$$n^{p-1} \equiv 1 \quad [p]$$

**Preuve (à connaître pour les ROC)** : D'après la propriété précédente,  $n^p - n$  est un multiple de  $p$ . Or,  $n^p - n = n(n^{p-1} - 1)$ .

Autrement dit,  $p$  est un diviseur de  $n(n^{p-1} - 1)$ . Par hypothèse,  $p$ , qui est un nombre premier, ne divise pas  $n$ . Donc  $n$  et  $p$  sont premiers entre eux. Par conséquent, d'après le Théorème de Gauss,  $p$  divise  $n^{p-1} - 1$ . On peut écrire cela ainsi :  $n^{p-1} - 1 \equiv 0[p]$ , c'est à dire  $n^{p-1} \equiv 1 \quad [p]$ . □

► **Exercice** : lire exercice corrigé page 53 (cryptographie)

► **Exercices** : 86p58 , 159p60